

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年4月2日(02.04.2020)



(10) 国際公開番号

WO 2020/066084 A1

(51) 国際特許分類:
G06F 21/55 (2013.01) G06Q 30/02 (2012.01)
(21) 国際出願番号: PCT/JP2019/015708
(22) 国際出願日: 2019年4月10日(10.04.2019)
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語
(30) 優先権データ:
特願 2018-179229 2018年9月25日(25.09.2018) JP

(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

(72) 発明者: 金井 文宏 (KANEI, Fumihito); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP). 〒

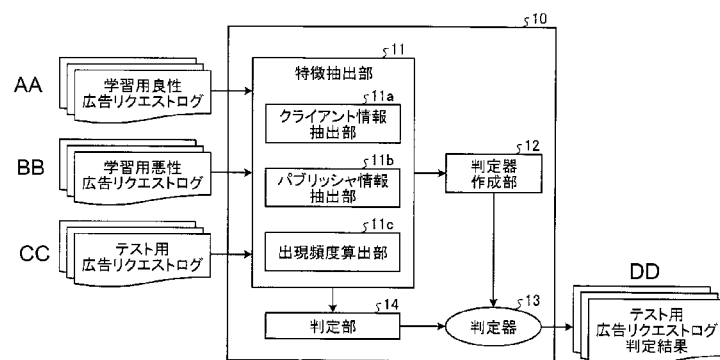
葉 大紀(CHIBA, Daiki); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP). 高田 雄太(TAKATA, Yuta); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP). 秋山 満昭(AKIYAMA, Mitsuaki); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP). 波戸 邦夫(HATO, Kunio); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH,

(54) Title: DETECTOR, DETECTION METHOD, AND DETECTION PROGRAM

(54) 発明の名称: 検知装置、検知方法および検知プログラム



11 Feature extraction unit
11a Client information extraction unit
11b Publisher information extraction unit
11c Appearance frequency calculation unit
12 Assessor creation unit
13 Assessor
14 Assessment unit
AA Benign advertising request log for learning
BB Malignant advertising request log for learning
CC Advertising request log for test
DD Assessment results for advertising request log for test

(57) Abstract: A feature extraction unit (11): extracts, from an advertising request requesting online advertising to be viewed, client information relating to a client who is the sender of the advertising request, and publisher information relating to a website of a publisher displaying the advertising; and calculates a prescribed feature amount for a plurality of advertising requests including at least a benign advertising request, in which the client information and the publisher information are used. An assessor creation unit (12) creates an assessor (13) for assessing whether or not an advertising request is malignant, using the calculated feature amount.

CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告 (条約第21条(3))

(57) 要約: 特徴抽出部 (11) が、オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出し、該クライアント情報と該パブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出し、判定器作成部 (12) が、算出された特徴量を用いて、広告リクエストが悪性か否かを判定する判定器 (13) を作成する。

明 細 書

発明の名称： 検知装置、検知方法および検知プログラム

技術分野

[0001] 本発明は、検知装置、検知方法および検知プログラムに関する。

背景技術

[0002] 近年、市場の発展に伴い、オンライン広告を標的とした広告不正の被害が深刻化している。オンライン広告は、Webサイトやモバイルアプリにおけるマネタイズ手段の一つである。オンライン広告においては、主に、エンドユーザ、パブリッシャ、広告主、および広告ネットワークの4種類のステークホルダーが存在する。

[0003] エンドユーザは、Webブラウザやモバイルアプリを介してオンライン広告を閲覧する。パブリッシャは、自身の管理するWebサイトやモバイルアプリ内に用意した広告表示枠を広告主に提供し、その対価に広告費を受け取る。広告主は、広告を出稿する。広告ネットワークは、パブリッシャと広告主との間のやり取りを仲介する役割を担う。

[0004] また、広告不正とは、実際には広告効果が発生しない手段を用いて、広告主が支払う広告費を浪費させる攻撃である。本来、Web広告は、ブラウザでWebサイトにアクセスしたエンドユーザ等の聴衆に閲覧され、クリックされるという想定のもとに表示される。これに対し、攻撃者は、広告効果が発生しない不正なWebトラフィックを発生させたり、自動的なクリックを発生させたりして、不正に広告費を詐取する。例えば、攻撃者は、アドウェアやPUP (Potentially Unwanted Program) 等をエンドユーザの用いる端末（クライアント）に感染させ、感染したクライアントから自動的な広告リクエストを発生させる。

[0005] このような広告不正への対策として、広告ネットワークの立場から、広告不正によって発生した広告リクエストを検知する技術が検討されている。例えば、広告不正により発生する広告リクエストや、広告リクエストによって

発生する広告収益が、正規のエンドユーザによる広告リクエストより高いバースト性を示すことを利用して、広告不正を検知する技術が開示されている（非特許文献1，2参照）。

先行技術文献

非特許文献

[0006] 非特許文献1：B.Stone-Gross, R.Stevens, A.Zarras, R.Kemmerer, C.Kruegel, and G.Vigna, “Understanding Fraudulent Activities in Online Ad Exchanges”, Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (IMC), 2011年, pp. 279–294

非特許文献2：V.Dave, S.Guha, and Y.Zhang, “ViceROI: Catching Click-Spam in Search Ad Networks”, Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2013年, pp.765–776

発明の概要

発明が解決しようとする課題

[0007] しかしながら、従来の技術では、攻撃者によって広告不正の検知が回避される場合がある。例えば、攻撃者は、自身の管理下にある多数のクライアントやパブリッシャサイトを用いて、分散的に広告不正を行うことが可能である。またその際に、攻撃者は、クライアントやパブリッシャサイトごとに、広告リクエスト数や広告リクエストにより発生する広告収益を任意に設定可能である。したがって、攻撃者が、広告リクエスト数や広告収益を正規のエンドユーザやパブリッシャサイトと同程度の値に設定した場合には、広告リクエストのバースト性に基づく従来の技術では、広告不正が検知されない。

[0008] 本発明は、上記に鑑みてなされたものであって、攻撃者に回避され難い広告不正の検知を行うことを目的とする。

課題を解決するための手段

[0009] 上述した課題を解決し、目的を達成するために、本発明に係る検知装置は、オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出し、該クライアント情報と該パブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出する抽出部と、算出された前記特徴量を用いて、広告リクエストが悪性か否かを判定する判定器を作成する判定器作成部と、を備えることを特徴とする。

発明の効果

[0010] 本発明によれば、攻撃者に回避され難い広告不正の検知を行うことが可能となる。

図面の簡単な説明

[0011] [図1]図1は、検知装置の概略構成を例示する模式図である。

[図2]図2は、広告リクエストログのデータ構成を例示する図である。

[図3]図3は、クライアント情報を説明するための説明図である。

[図4]図4は、パブリッシャ情報を説明するための説明図である。

[図5]図5は、特徴抽出部の処理を説明するための説明図である。

[図6]図6は、特徴抽出部の処理を説明するための説明図である。

[図7]図7は、検知処理手順を示すフローチャートである。

[図8]図8は、特徴抽出処理手順を示すフローチャートである。

[図9]図9は、検知プログラムを実行するコンピュータの一例を示す図である。

発明を実施するための形態

[0012] 以下、図面を参照して、本発明の一実施形態を詳細に説明する。なお、この実施形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。

[0013] [検知装置の構成]

図1は、検知装置の概略構成を例示する模式図である。検知装置10では

、汎用コンピュータのCPU（Central Processing Unit）等を用いて実現される制御部が、図1に示すように、特徴抽出部11、判定器作成部12、および判定部14として機能する。なお、これらの機能部は、それぞれあるいは一部が異なるハードウェアに実装されてもよい。例えば、判定部14は、特徴抽出部11および判定器作成部12とは異なるハードウェアに実装されてもよい。

[0014] また、検知装置10では、RAM（Random Access Memory）、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される記憶部に、判定器13が記憶される。

[0015] 特徴抽出部11は、抽出部として機能する。すなわち、特徴抽出部11は、オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出する。また、特徴抽出部11は、このクライアント情報とこのパブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出する。

[0016] 具体的には、まず、特徴抽出部11は、図示しないキーボード等の入力部あるいはNIC（Network Interface Card）等の通信制御部を介して、オンライン広告の閲覧を要求する広告リクエストの入力を受け付ける。ここで、図2は、広告リクエストのデータ構成を例示する図である。図2に示すように、広告リクエストには、クライアントIPアドレス、ユーザエージェント、およびパブリッシャURL等が含まれる。

[0017] クライアントIPアドレスは、広告を閲覧するエンドユーザが使用するクライアント、すなわち広告リクエストの送信元であるクライアントのIPアドレスである。ユーザエージェントとは、クライアントで広告の閲覧に使用されているソフトウェアまたはハードウェア等のユーザエージェントである。パブリッシャURLは、広告が表示されたパブリッシャのウェブサイトの

URLである。

[0018] なお、後述する判定器作成部12は、学習用の広告リクエストを用いて処理を行う。学習用の広告リクエストとしては、学習用悪性広告リクエストログと、学習用良性広告リクエストログとが用いられる。学習用悪性広告リクエストログとは、広告不正によって発生した悪性な広告リクエストのログである。また、学習用良性広告リクエストログとは、正規のエンドユーザの活動によって発生した良性な広告リクエストのログである。

[0019] また、後述する判定部14は、テスト用の広告リクエストであるテスト用広告リクエストログを用いて処理を行う。テスト用広告リクエストログとは、悪性か否かの判定対象の広告リクエストのログである。

[0020] 図1の説明に戻る。特徴抽出部11は、クライアント情報抽出部11a、パブリッシャ情報抽出部11b、および出現頻度算出部11cを含む。

[0021] クライアント情報抽出部11aは、広告リクエストの送信元であるクライアントに関するクライアント情報を抽出する。ここで、図3は、クライアント情報を説明するための図である。

[0022] 例えば、クライアント情報抽出部11aは、クライアント情報として、図3(a)に示すように、広告リクエストの送信元のIPアドレスが属するネットワークの情報を抽出する。具体的には、クライアント情報抽出部11aは、広告リクエストに含まれるクライアントIPアドレスを用いて、このIPアドレスからドメイン名を解決するDNS逆引きを行う。そして、クライアント情報抽出部11aは、DNS逆引き結果のドメイン名から、インターネット上でユーザの希望により登録可能な部分の最小単位を表す部分文字列（以下、*rDNS-e2LD*と記す。）を抽出し、これをクライアント情報とする。

[0023] 例えば、クライアント情報抽出部11aは、周知のPublic Suffix Listを参照して、ドメイン名から、*rDNS-e2LD*を抽出する。Public Suffixは、ドメイン名の上位の個人のユーザがコントロールできない文字列を表す。したがって、クライアント情報抽出部11aは、ドメイン名に含まれるP

ublic Suffixの1レベル下位の部分までを、rDNS-e2LDとして抽出すればよい。

[0024] 図3(a)に示す例では、Public Suffixに「.example」が含まれている場合に、クライアント情報抽出部11aは、DNS逆引き結果のドメインから、rDNS-e2LDとして「ispX.example」や「ispY.example」を抽出している。

[0025] クライアント情報抽出部11aは、クライアント情報として、図3(b)に示すように、クライアントの動作環境に関する情報を抽出してもよい。具体的には、クライアント情報抽出部11aは、広告リクエストに含まれるユーザエージェントを用いて、ユーザエージェントが表すOSの種別とメジャーバージョン番号とを連結した文字列（以下、OS-versionと記す。）を抽出し、これをクライアント情報とする。

[0026] 例えば、クライアント情報抽出部11aは、予めOSの種別やバージョンごとにシグネチャを定義しておき、ユーザエージェントを表す文字列に対してシグネチャマッチングを行う。すなわち、クライアント情報抽出部11aは、ユーザエージェントに対応するシグネチャを特定することにより、ユーザエージェントを表すOSの種別とバージョン番号とを抽出する。なお、クライアント情報抽出部11aは、例えば、オープンソースソフトウェアであるuap-coreを用いて、シグネチャを定義することができる。

[0027] 図3(b)に示す例では、クライアント情報抽出部11aは、ユーザエージェントを表す文字列「aaaa/5.0(bbbb NT 6.1;…」から、OS-version「bbbb7」を抽出している。

[0028] パブリッシャ情報抽出部11bは、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報を抽出する。ここで、図4は、パブリッシャ情報を説明するための図である。例えば、パブリッシャ情報抽出部11bは、パブリッシャ情報として、図4に示すように、パブリッシャのウェブサイトのドメイン名を抽出する。具体的には、パブリッシャ情報抽出部11bは、広告リクエストに含まれるパブリッシャURLから、パブリッシャサイ

トのFQDN (Fully Qualified Domain Name) を抽出し、これをパブリッシャ情報とする。

[0029] パブリッシャ情報抽出部11bは、URLから「http://」、「https://」等のスキームを表す部分と、「/」等の区切り文字以降のパス名を表す部分とを除外することにより、FQDNを抽出することができる。図4に示す例では、パブリッシャ情報抽出部11bは、パブリッシャURL「https://example.com/…」からFQDN「example.com」を抽出している。

[0030] 出現頻度算出部11cは、クライアント情報とパブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出する。例えば、出現頻度算出部11cは、クライアント情報およびパブリッシャ情報の、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する出現頻度を用いて特徴量を算出する。

[0031] ここで、図5および図6は、特徴抽出部11の処理を説明するための説明図である。まず、図5には、クライアント情報およびパブリッシャ情報の出現頻度の算出処理について、例示されている。

[0032] 図5(a)に例示する広告リクエストから、図5(b)に示すように、クライアント情報抽出部11aがクライアント情報を抽出し、パブリッシャ情報抽出部11bがパブリッシャ情報を抽出する。

[0033] 図5(b)に示す例では、パブリッシャ情報抽出部11bは、パブリッシャ情報として、FQDNを抽出している。また、クライアント情報抽出部11aは、クライアント情報として、rDNS-e2LDとOS-versionとを抽出している。なお、クライアント情報およびパブリッシャ情報は、これに限定されない。例えば、クライアント情報抽出部11aは、rDNS-e2LD、OS-versionのいずれか一方のみを、クライアント情報として抽出してもよい。

[0034] 次に、図5(c)に示すように、出現頻度算出部11cが、クライアント情報およびパブリッシャ情報の出現頻度を算出する。具体的には、出現頻度算出部11cは、まず、図5(b)に示した各広告リクエストのクライアン

ト情報およびパブリッシャ情報を集計する。例えば、出現頻度算出部11cは、`rDNS-e2LD`、`OS-version`、`FQDN`のそれぞれについて、全広告リクエストに出現するユニークな値の一覧を取得する。また、出現頻度算出部11cは、`rDNS-e2LD`と`FQDN`、`rDNS-e2LD`と`OS-version`、`OS-version`と`FQDN`の3種の組み合わせのそれぞれについて、同一の広告リクエストに出現するユニークな値の組み合わせの一覧を取得する。

[0035] そして、出現頻度算出部11cは、取得した一覧のそれぞれの値または値の組み合わせについて、図5(a)に示した全広告リクエスト中に出現した出現頻度を算出する。なお、出現頻度は、全広告リクエストにおける出現回数でもよいし、出現回数を0から1の間で正規化した値でもよい。図5(c)に示す例では、その双方が算出されている。例えば、`OS-version`「bbbb7」と`FQDN`「example.net」との組み合わせは、全広告リクエストにおける出現回数が2回であり、出現頻度は2、正規化後の出現頻度は0.285と算出されている。

[0036] 次に、出現頻度算出部11cは、算出した出現頻度を用いて特徴量を算出する。ここで、図6には、図5に示したように算出された出現頻度を用いた特徴量の算出処理が例示されている。図6に示すように、出現頻度算出部11cは、算出された出現頻度を用いて、各広告リクエストの特徴量として、各広告リクエストのクライアント情報およびパブリッシャ情報の出現頻度を成分とする特徴ベクトルを生成する。

[0037] 例えば、図6(b)に示す広告リクエストから、図6(c)に示すように抽出されたクライアント情報およびパブリッシャ情報について、図6(a)に示すように算出された出現頻度を成分として、図6(d)に示すように特徴ベクトルを生成する。

[0038] 図6に示す例では、各広告リクエストについての特徴ベクトルは、(`rDNS-e2LD`、`OS-version`、`FQDN`、`rDNS-e2LD`と`FQDN`、`rDNS-e2LD`と`OS-version`、`OS-versi`

onとFQDN)の順に、各値の出現頻度を成分として生成されている。なお、この順は特に限定されず、全広告リクエストについて共通であればよい。

[0039] 例えば、図6(d)に示す特徴ベクトルは、図6(a)に網掛けで示された正規化後の出現頻度の値を成分として生成される6次元のベクトルである。すなわち、この特徴ベクトルは、図6(b)に示した広告リクエストログのレコードのrDNS-e2LD「ispX.example」、OS-version「bbbb7」、FQDN「example.com」、およびそれらの組み合わせの出現頻度を用いて生成されている。

[0040] このように、特徴抽出部11は、良性な広告リクエストを含む多数の広告リクエストに対する特徴量を算出する。すなわち、特徴抽出部11は、正規のエンドユーザによって発生する広告リクエストの統計的な傾向を用いて、各広告リクエストの特徴量を算出する。攻撃者は、正規のエンドユーザによって発生する統計的な傾向を操作することは困難であるため、このような良性な広告リクエストを含む多数の広告リクエストに対する特徴量は、攻撃者が操作することが困難な値である。

[0041] 判定器作成部12は、算出された特徴量を用いて、広告リクエストが悪性か否かを判定する判定器13を作成する。具体的には、例えば、判定器作成部12は、学習用悪性広告リクエストログから算出された悪性な特徴ベクトルと、学習用良性広告リクエストログから算出された良性な特徴ベクトルとを用いて、悪性な広告リクエストへの悪性ラベルの付与を学習する。これにより、判定器作成部12は、広告リクエストに悪性ラベル／良性ラベルのいずれかを付与する判定器13を作成する。

[0042] 判定部14は、作成された判定器13を用いて、広告リクエストが悪性か否かを判定する。具体的には、判定部14は、テスト用広告リクエストログについて特徴抽出部11が算出した所定の特徴量を判定器13に入力する。なお、例えば、テスト用広告リクエストログに含まれるレコード数が少ない場合等には、特徴抽出部11の出現頻度算出部11cは、学習用広告リクエ

ストログについて算出された出願頻度値を適用して、各広告リクエストの特徴量を算出してもよい。

[0043] 判定器 1 3 がテスト用広告リクエストログに悪性ラベルを付与した場合に、判定部 1 4 は、当該テスト用広告リクエストが悪性と判定する。また、判定器 1 3 がテスト用広告リクエストログに良性ラベルを付与した場合に、判定部 1 4 は、当該テスト用広告リクエストが良性、すなわち悪性ではないと判定する。

[0044] [検知処理]

次に、図 7 および図 8 を参照して、本実施形態に係る検知装置 1 0 による検知処理について説明する。図 7 は、検知処理手順を示すフローチャートである。図 7 のフローチャートは、例えば、ユーザが検知処理の開始を指示する操作入力を行ったタイミングで開始される。

[0045] まず、特徴抽出部 1 1 が、広告リクエストログの入力を受け付けた場合に（ステップ S 1）、各広告リクエストについて、特徴抽出処理を行う。すなわち、特徴抽出部 1 1 は、クライアント情報とパブリッシャ情報とを用いた、入力された全広告リクエストに対する所定の特徴量を算出する（ステップ S 2）。

[0046] 判定器作成部 1 2 は、学習用広告リクエストログについて算出された特徴量を用いて、広告リクエストログが悪性か否かを判定する判定器 1 3 を作成する（ステップ S 3）。すなわち、判定器作成部 1 2 は、学習用悪性広告リクエストログから算出された悪性な特徴量と、学習用良性広告リクエストログから算出された良性な特徴量とを用いて、広告リクエストに悪性ラベル／良性ラベルのいずれかを付与する判定器 1 3 を作成する。

[0047] また、判定部 1 4 は、テスト用広告リクエストログについて算出された特徴量を、作成された判定器 1 3 に入力することにより、テスト用広告リクエストログが悪性か否かを判定する（ステップ S 4）。これにより、一連の検知処理が終了する。

[0048] また、図 8 は、特徴抽出処理（上記ステップ S 2）手順を示すフローチャ

ートである。特徴抽出部 11 において、クライアント情報抽出部 11 a が、広告リクエストからクライアントを表すクライアント情報を抽出する。そして、出現頻度算出部 11 c が、入力された全広告リクエストに出現するクライアント情報のユニークな値の一覧を取得する（ステップ S 2 1）。

[0049] また、パブリッシャ情報抽出部 11 b が、広告リクエストからパブリッシャウェブサイトを表すパブリッシャ情報を抽出する。そして、出現頻度算出部 11 c が、入力された全広告リクエストに出現するパブリッシャ情報のユニークな値の一覧を取得する（ステップ S 2 2）。

[0050] また、出現頻度算出部 11 c は、同一の広告リクエストに出現するクライアント情報およびパブリッシャ情報のユニークな値の組み合わせの一覧を取得する（ステップ S 2 3）。

[0051] 出現頻度算出部 11 c は、取得した一覧から順次、値または値の組み合わせを選択し（ステップ S 2 4）、選択した値または値の組み合わせについて、特徴量として、全広告リクエスト中に出現した出現頻度を算出する（ステップ S 2 5）。

[0052] 出現頻度算出部 11 c は、一覧の値または値の組み合わせについて出現頻度を算出する処理を繰り返す（ステップ S 2 6、N o → ステップ S 2 4）。そして、出現頻度算出部 11 c は、一覧の値または値の組み合わせの全てについて出現頻度を算出した場合に（ステップ S 2 6、Y e s）、一連の特徴抽出処理を終了する。

[0053] 以上、説明したように、本実施形態の検知装置 10 において、特徴抽出部 11 が、オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出し、該クライアント情報と該パブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出する。また、判定器作成部 12 が、算出された特徴量を用いて、広告リクエストが悪性か否かを判定する判定器 13 を作成する。

[0054] ここで、従来は、例えば、広告閲覧ユーザおよびパブリッシャサイトごとに発生した広告リクエスト数やCTR (Click Through Rate) を計測し、計測値のバースト性を元に広告不正を検知していた（非特許文献1参照）。また、広告不正によって発生する広告収益が、通常のパブリッシャが発生させる広告収益と比較して高いことにより広告不正を検知していた（非特許文献2参照）。このように、従来、広告不正により発生する広告リクエストや、広告リクエストによって発生する広告収益が、正規のエンドユーザによる広告リクエストより高いバースト性を示すことを利用して、広告不正を検知していた。

[0055] これに対し、本実施形態の検知装置10では、特徴抽出部11が、各広告リクエストについて、正規のエンドユーザによって発生する良質な広告リクエストを含む多数の広告リクエストに対する特徴量を算出する。すなわち、特徴抽出部11は、良質な広告リクエストの統計的な傾向を用いて、各広告リクエストの特徴量を算出する。例えば、特徴抽出部11は、クライアント情報およびパブリッシャ情報の、正規のエンドユーザによって発生する良質な広告リクエストを含む多数の広告リクエストに対する出現頻度を用いて特徴量を算出する。

[0056] なお、特徴抽出部11は、クライアント情報として、例えば、広告リクエストの送信元のIPアドレスが属するネットワークの情報を抽出し、これを用いて特徴量を算出する。あるいは、特徴抽出部11は、クライアント情報として、クライアントの動作環境に関する情報を抽出し、これを用いて特徴量を算出する。また、特徴抽出部11は、パブリッシャ情報として、パブリッシャのウェブサイトのドメイン名を抽出し、これを用いて特徴量を算出する。

[0057] 攻撃者は、正規のエンドユーザによって発生する統計的な傾向を操作することは困難である。たとえ攻撃者が多数のクライアントやパブリッシャウェブサイトを用いて攻撃を行った場合にも、これらの特徴量を正規のエンドユーザによる広告リクエストと同様の値になるように設定することは困難であ

る。したがって、このような良質な広告リクエストを含む多数の広告リクエストに対する特徴量は、攻撃者が操作することは困難な値である。

[0058] このように、本実施形態の検知装置 10 は、攻撃者が操作することが困難な特徴量を用いて、広告リクエストが悪性か否かを判定する判定器 13 を作成する。ここで作成された判定器 13 を用いて、判定部 14 が、広告リクエストが悪性か否かを判定する。したがって、検知装置 10 は、攻撃者が回避し難い広告不正の検知を行うことが可能となる。

[0059] [プログラム]

上記実施形態に係る検知装置 10 が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。一実施形態として、検知装置 10 は、パッケージソフトウェアやオンラインソフトウェアとして上記の検知処理を実行する検知プログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記の検知プログラムを情報処理装置に実行させることにより、情報処理装置を検知装置 10 として機能させることができる。ここで言う情報処理装置には、デスクトップ型またはノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはスマートフォン、携帯電話機や PHS (Personal Handyphone System) などの移動体通信端末、さらには、PDA (Personal Digital Assistant) などのスレート端末などがその範疇に含まれる。また、検知装置 10 の機能を、クラウドサーバに実装してもよい。

[0060] 図 9 は、検知プログラムを実行するコンピュータの一例を示す図である。コンピュータ 1000 は、例えば、メモリ 1010 と、CPU 1020 と、ハードディスクドライブインタフェース 1030 と、ディスクドライブインタフェース 1040 と、シリアルポートインタフェース 1050 と、ビデオアダプタ 1060 と、ネットワークインタフェース 1070 とを有する。これらの各部は、バス 1080 によって接続される。

[0061] メモリ 1010 は、ROM (Read Only Memory) 1011 および RAM 1012 を含む。ROM 1011 は、例えば、BIOS (Basic Input Out

put System) 等のブートプログラムを記憶する。ハードディスクドライブインタフェース 1030 は、ハードディスクドライブ 1031 に接続される。ディスクドライブインタフェース 1040 は、ディスクドライブ 1041 に接続される。ディスクドライブ 1041 には、例えば、磁気ディスクや光ディスク等の着脱可能な記憶媒体が挿入される。シリアルポートインタフェース 1050 には、例えば、マウス 1051 およびキーボード 1052 が接続される。ビデオアダプタ 1060 には、例えば、ディスプレイ 1061 が接続される。

[0062] ここで、ハードディスクドライブ 1031 は、例えば、OS 1091、アプリケーションプログラム 1092、プログラムモジュール 1093 およびプログラムデータ 1094 を記憶する。上記実施形態で説明した各情報は、例えばハードディスクドライブ 1031 やメモリ 1010 に記憶される。

[0063] また、検知プログラムは、例えば、コンピュータ 1000 によって実行される指令が記述されたプログラムモジュール 1093 として、ハードディスクドライブ 1031 に記憶される。具体的には、上記実施形態で説明した検知装置 10 が実行する各処理が記述されたプログラムモジュール 1093 が、ハードディスクドライブ 1031 に記憶される。

[0064] また、検知プログラムによる情報処理に用いられるデータは、プログラムデータ 1094 として、例えば、ハードディスクドライブ 1031 に記憶される。そして、CPU 1020 が、ハードディスクドライブ 1031 に記憶されたプログラムモジュール 1093 やプログラムデータ 1094 を必要に応じて RAM 1012 に読み出して、上述した各手順を実行する。

[0065] なお、検知プログラムに係るプログラムモジュール 1093 やプログラムデータ 1094 は、ハードディスクドライブ 1031 に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ 1041 等を介して CPU 1020 によって読み出されてもよい。あるいは、検知プログラムに係るプログラムモジュール 1093 やプログラムデータ 1094 は、LAN や WAN (Wide Area Network) 等のネットワークを介して

接続された他のコンピュータに記憶され、ネットワークインタフェース 1070 を介して CPU 1020 によって読み出されてもよい。

[0066] 以上、本発明者によってなされた発明を適用した実施形態について説明したが、本実施形態による本発明の開示の一部をなす記述および図面により本発明は限定されることはない。すなわち、本実施形態に基づいて当業者等によりなされる他の実施形態、実施例および運用技術等は全て本発明の範疇に含まれる。

符号の説明

- [0067] 10 検知装置
 - 11 特徴抽出部
 - 11a クライアント情報抽出部
 - 11b パブリッシャ情報抽出部
 - 11c 出現頻度算出部
 - 12 判定器作成部
 - 13 判定器
 - 14 判定部

請求の範囲

- [請求項1] オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出し、該クライアント情報と該パブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出する抽出部と、
- 算出された前記特徴量を用いて、広告リクエストが悪性か否かを判定する判定器を作成する判定器作成部と、
- を備えることを特徴とする検知装置。
- [請求項2] 前記抽出部は、前記クライアント情報として、前記広告リクエストの送信元のIPアドレスが属するネットワークの情報を抽出し、前記特徴量を算出することを特徴とする請求項1に記載の検知装置。
- [請求項3] 前記抽出部は、前記クライアント情報として、前記クライアントの動作環境に関する情報を抽出し、前記特徴量を算出することを特徴とする請求項1に記載の検知装置。
- [請求項4] 前記抽出部は、前記パブリッシャ情報として、前記パブリッシャのウェブサイトのドメイン名を抽出し、前記特徴量を算出することを特徴とする請求項1に記載の検知装置。
- [請求項5] 前記抽出部は、前記クライアント情報および前記パブリッシャ情報の前記複数の広告リクエストに対する出現頻度を用いて前記特徴量を算出することを特徴とする請求項1に記載の検知装置。
- [請求項6] 検知装置で実行される検知方法であって、
- オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出し、該クライアント情報と該パブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対す

る所定の特徴量を算出する抽出工程と、

算出された前記特徴量を用いて、広告リクエストが悪性か否かを判定する判定器を作成する判定器作成工程と、

を含んだことを特徴とする検知方法。

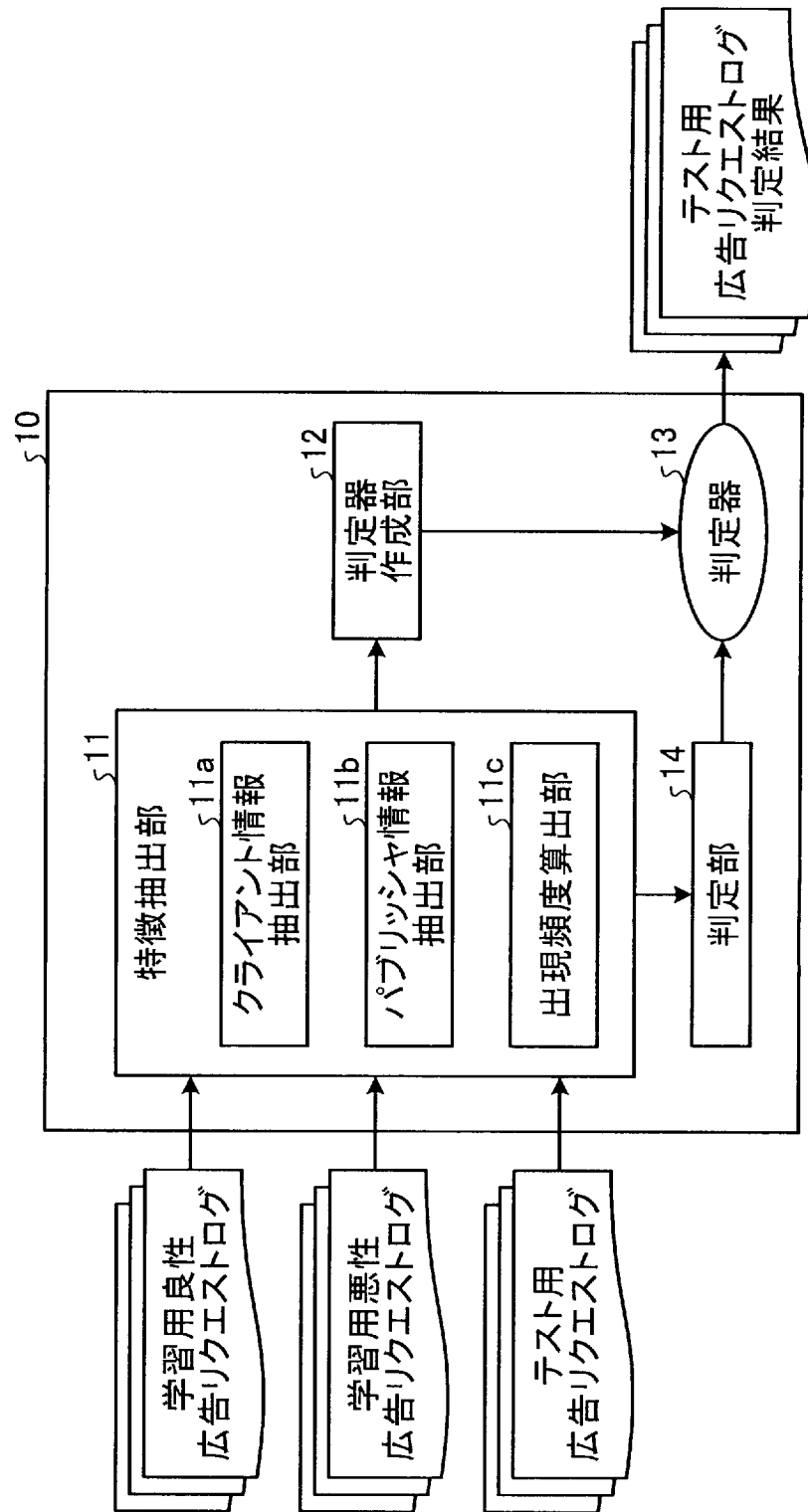
[請求項7]

オンライン広告の閲覧を要求する広告リクエストから、該広告リクエストの送信元であるクライアントに関するクライアント情報と、広告を表示するパブリッシャのウェブサイトに関するパブリッシャ情報とを抽出し、該クライアント情報と該パブリッシャ情報とを用いた、少なくとも良質な広告リクエストを含む複数の広告リクエストに対する所定の特徴量を算出する抽出ステップと、

算出された前記特徴量を用いて、広告リクエストが悪性か否かを判定する判定器を作成する判定器作成ステップと、

をコンピュータに実行させるための検知プログラム。

[図1]



[図2]

クライアントIPアドレス	ユーザエージェント	パブリッシャURL
198.51.100.15	aaaaa/5.0 (bbbb NT 6.1; ...	https://example.com/...
203.0.113.20	aaaaa/5.0 (cccc; dddd 6.0; ...	https://example.org/...
...	...	...

[図3]

(a)

クライアントIPアドレス	DNS逆引き結果	クライアント情報 (rDNS-e2LD)
198.51.100.15	15-100-51-198.ispX.example	ispX.example
203.0.113.20	20.113.0.203.ispY.example	ispY.example
...	...	...

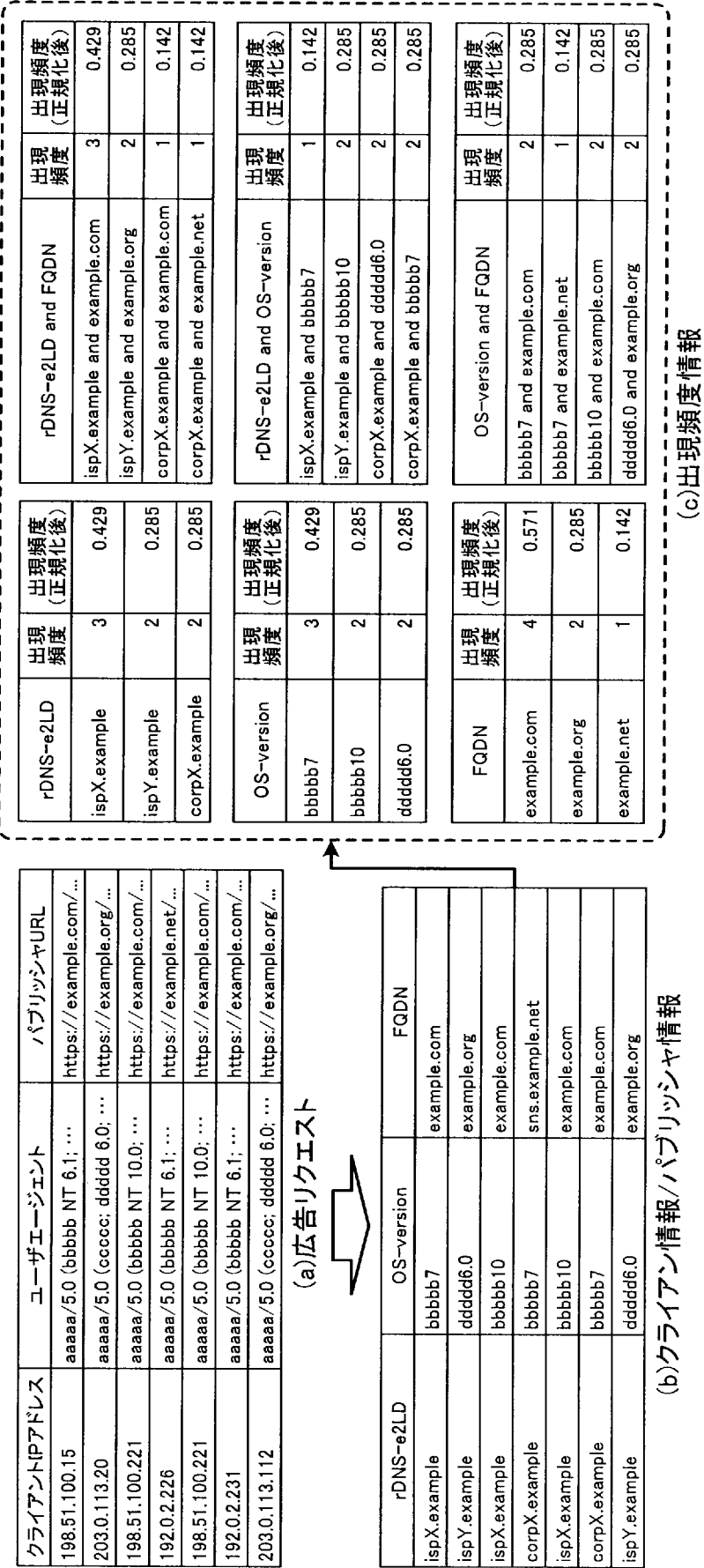
(b)

ユーザエージェント	クライアント情報 (OS-version)
aaaaa/5.0 (bbbb NT 6.1; ...	bbbb7
aaaaa/5.0 (cccc; dddd 6.0; ...	dddd6.0
...	...

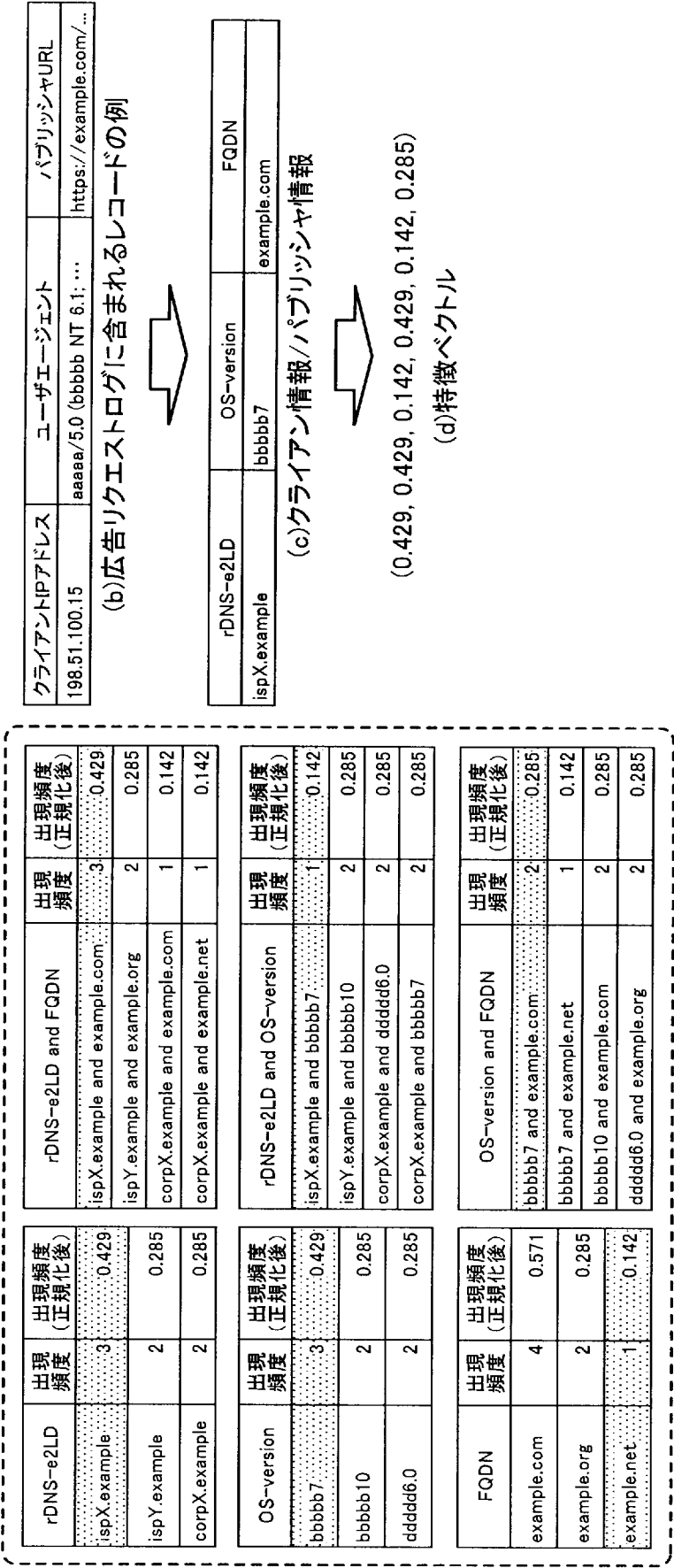
[図4]

パブリッシャURL	パブリッシャ情報 (FQDN)
https://example.com/...	example.com
https://example.org/...	example.org
...	...

[図5]



[図6]



クライアントIPアドレス	ユーザーエージェント	パブリッシュURL
198.51.100.15	aaaaa/5.0 (bbbb NT 6.1; ...	https://example.com/ ...

(b)広告リクエストログに含まれるレコードの例

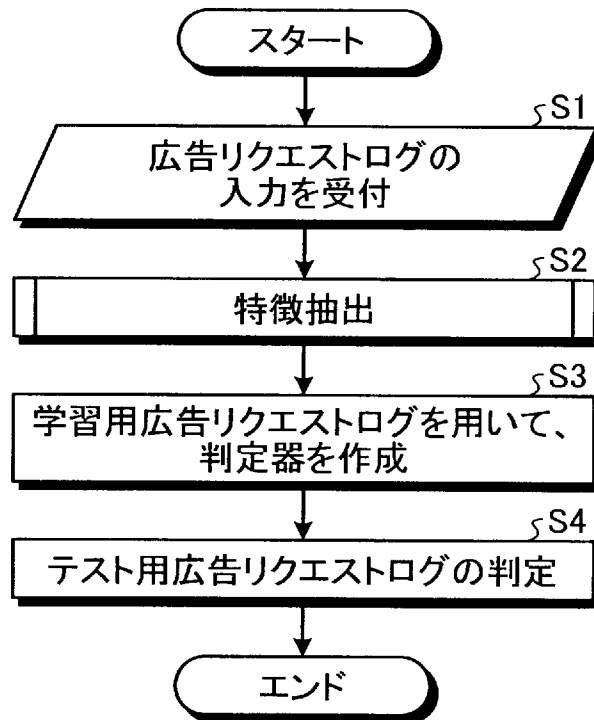
rDNS-e2LD	OS-version	FQDN
ispX.example	bbbb7	example.com

(c)クライアント情報/パブリッシュ情報

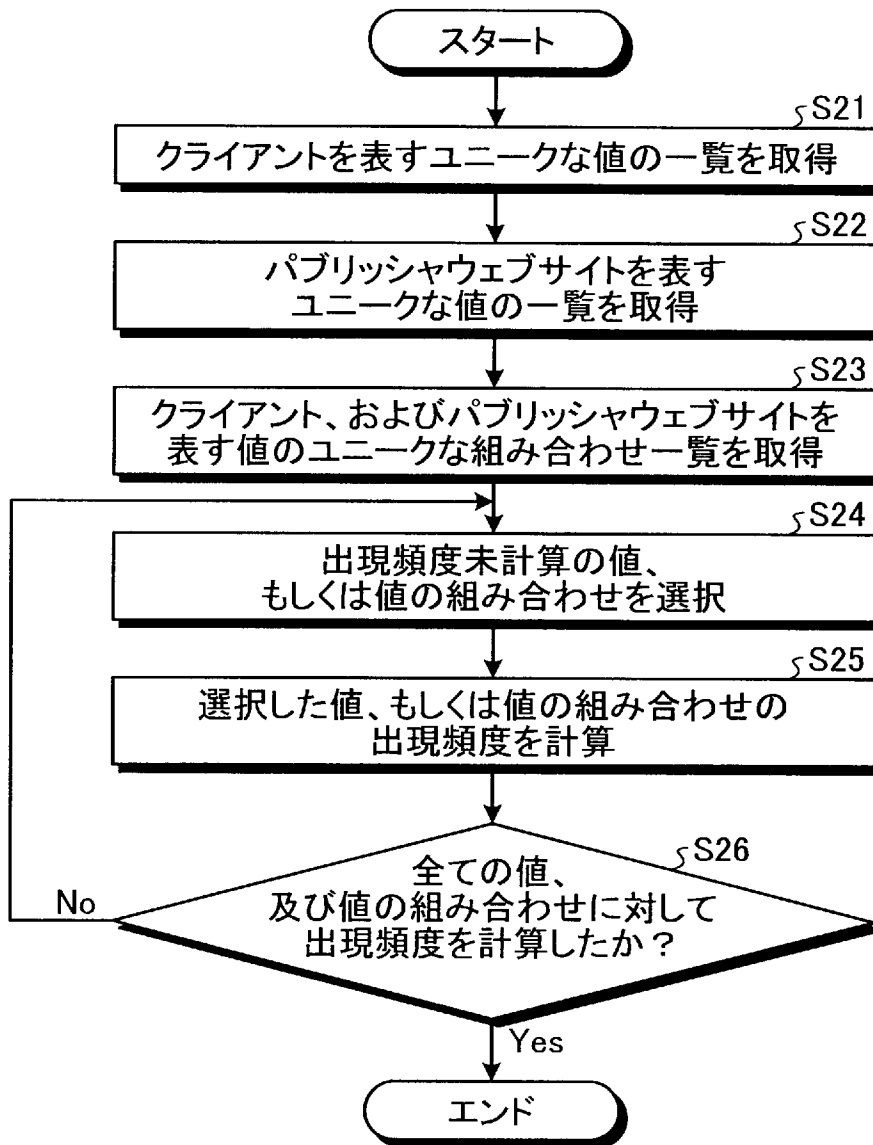
(0.429, 0.429, 0.142, 0.429, 0.142, 0.285)

(d)特徴ベクトル

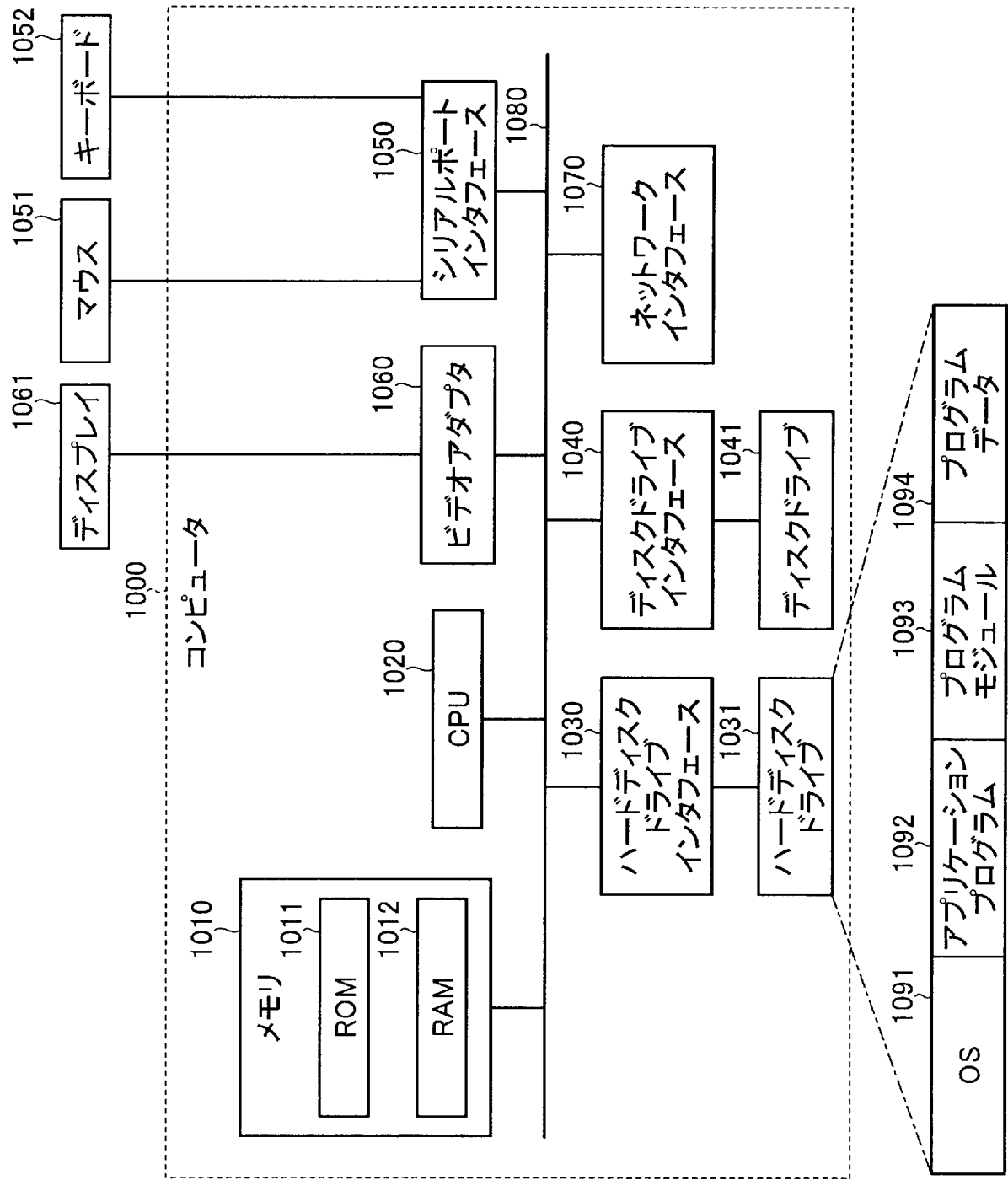
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/015708

A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. G06F21/55 (2013.01) i, G06Q30/02 (2012.01) i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int. Cl. G06F21/55, G06Q30/02 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2019 Registered utility model specifications of Japan 1996-2019 Published registered utility model applications of Japan 1994-2019 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore, advertisement, fraud, machine learning		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	HAIDER, C. M. R. et al., An ensemble learning based approach for impression fraud detection in mobile advertising, Journal of Network and Computer Applications, [online], 27 March 2018, vol. 112, pp. 126-141, [retrieved on 06 July 2019], retrieved from the Internet <URL: https://www.sciencedirect.com/science/article/pii/S1084804518300729?via%3Dihub >, <DOI:10.1016/j.jnca.2018.02.021>, especially 1. Introduction, 3. Mobile advertisement ecosystem, 4. Our Approach	1, 2, 5-7 3, 4
☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 08.07.2019		Date of mailing of the international search report 16.07.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/015708

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	金井文宏他, 広告ネットワーク上で観測されたユーザアクティビティの分析による広告不正の実態調査, 電子情報通信学会技術研究報告, 28 February 2018, vol. 117, no. 481, pp. 97-102, in particular, 3. Data Set, 4. Data Analysis, 5. Discussion, 7. Conclusion (KANEI, Fumihiko et al. An Empirical Analysis of Online Advertising Fraud by analyzing User Activities Observed in the Ad Network. IEICE Technical Report.)	3, 4
A	US 2018/0253755 A1 (TENCENT TECHNOLOGY(SHENZHEN)COMPANY LIMITED) 06 September 2018, paragraphs [0043]-[0051], [0070]-[0179]	1-7
A	US 2010/0082400 A1 (YAHOO! INC.) 01 April 2010, paragraphs [0017]-[0041]	1-7
A	JP 2008-135030 A (NHN CORP.) 12 June 2008, paragraphs [0021]-[0076]	1-7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2019/015708

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
US 2018/0253755 A1	2018.09.06	JP 2018-536956 A WO 2017/202336 A1 CN 106022834 A	2018.12.13 2017.11.30 2016.10.12
US 2010/0082400 A1	2010.04.01	Family: none	
JP 2008-135030 A	2008.06.12	US 2008/0126159 A1, paragraphs [0031] - [0086] KR 10-2008-0048185 A	2008.05.29 2008.06.02

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. G06F21/55(2013.01)i, G06Q30/02(2012.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. G06F21/55, G06Q30/02

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore
advertisement, fraud, machine learning

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X Y	HAIDER, C. M. R., et al., An ensemble learning based approach for impression fraud detection in mobile advertising, Journal of Network and Computer Applications, [online], 2018.03.27, Vol.112, p.126-141, [retrieved on 2019.07.06], retrieved from the Interenet <URL:https://www.sciencedirect.com/science/article/pii/S1084804518300729?via%3Dihub>, <DOI:10.1016/j.jnca.2018.02.021>, especially 1. Introduction, 3. Mobile advertisement ecosystem, 4. Our Approach	1, 2, 5-7 3, 4

☒ C欄の続きにも文献が列挙されている。☒ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

08.07.2019

国際調査報告の発送日

16.07.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5 S

9364

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	金井文宏 他, 広告ネットワーク上で観測されたユーザアクティビティの分析による広告不正の実態調査, 電子情報通信学会技術研究報告, 2018.02.28, 第117巻 第481号, p.97-102, 特に 3.データセット, 4.データ分析, 5.議論, 7.おわりに	3, 4
A	US 2018/0253755 A1 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 2018.09.06, 段落[0043]-[0051], [0070]-[0179]	1-7
A	US 2010/0082400 A1 (YAHOO! INC..) 2010.04.01, 段落[0017]-[0041]	1-7
A	JP 2008-135030 A (エヌエイチエヌ コーポレーション) 2008.06.12, 段落[0021]-[0076]	1-7

国際調査報告
 パテントファミリーに関する情報

国際出願番号 PCT/J P 2 0 1 9 / 0 1 5 7 0 8

US 2018/0253755 A1	2018. 09. 06	JP 2018-536956 A	2018. 12. 13
		WO 2017/202336 A1	2017. 11. 30
		CN 106022834 A	2016. 10. 12
US 2010/0082400 A1	2010. 04. 01	ファミリーなし	
JP 2008-135030 A	2008. 06. 12	US 2008/0126159 A1, 段落[0031]-[0086]	2008. 05. 29
		KR 10-2008-0048185 A	2008. 06. 02